

BUILDING A ZERO TRUST ARCHITECTURE

Natalio Pincever
Sr. Director, Product Management Federal Gov

Geoffrey Carlisle
Solution Architect , Product Management Federal Gov

ZEROTRUST



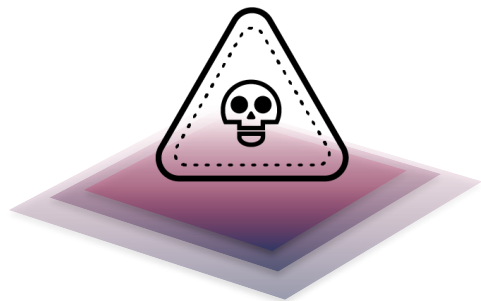
TRUST IS A DANGEROUS VULNERABILITY

THAT IS **EXPLOITED** BY MALICIOUS ACTORS

ZERO TRUST

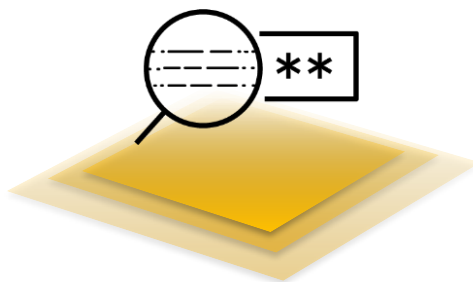
Zero Trust is a security model that prevents breaches by eliminating assumed trust in the digital world and instead consistently verifies all traffic from all users, devices, and applications at all locations

A Zero Trust Strategy Reduces Attack Opportunities



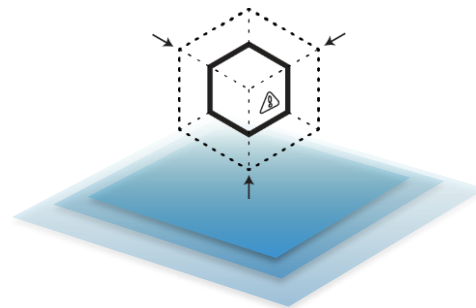
Problem

Broken trust model
exploited by hackers



Action

Build a zero
trust network



Benefit

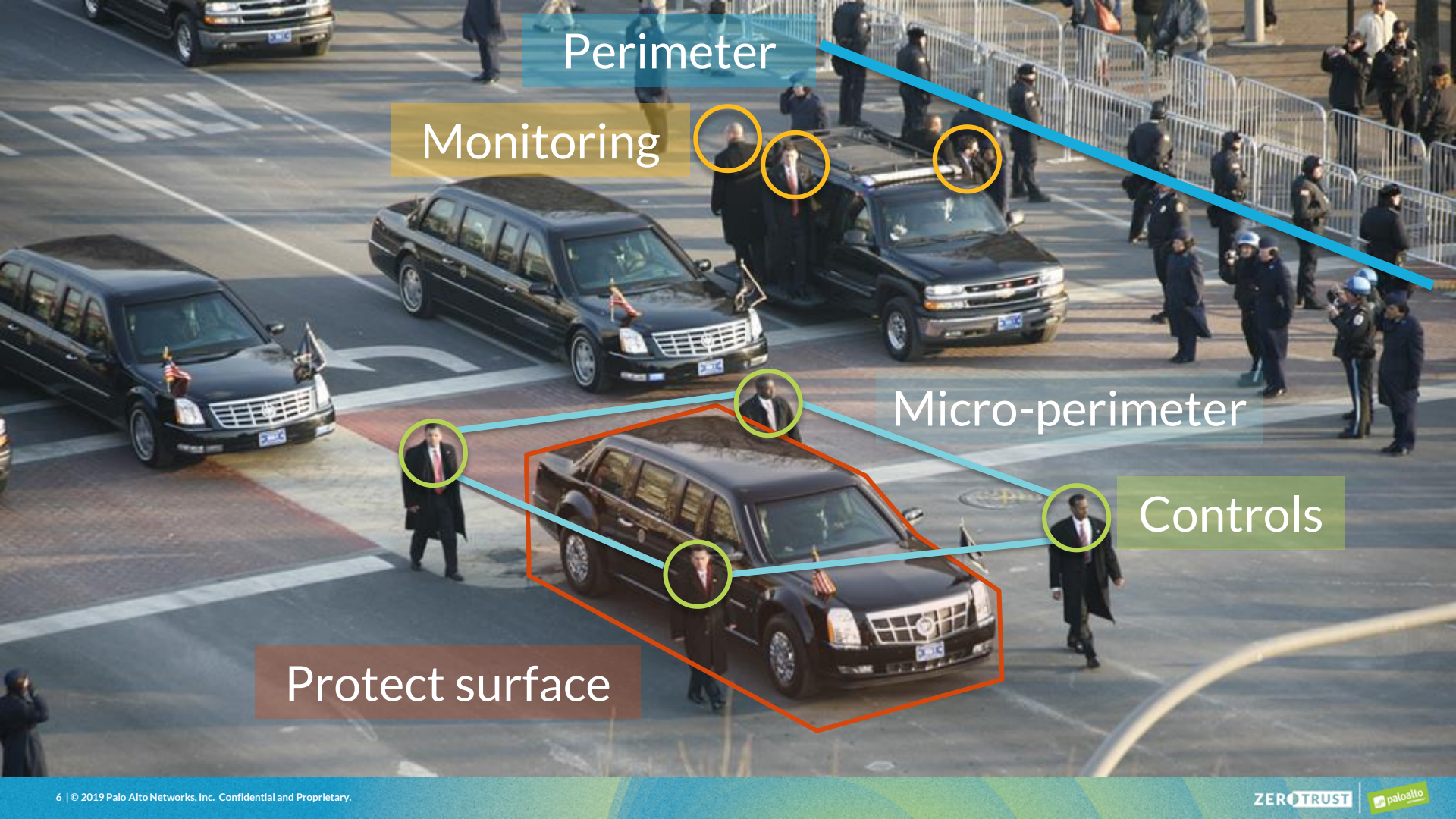
Helps stop
data breaches

An aerial photograph of a presidential motorcade. Several black limousines are moving through a city street. They are surrounded by a large number of Secret Service agents in dark suits and police officers in uniform. Metal barricades line the sidewalks, and a crowd of people is visible in the background. The scene is captured from a high angle, showing the layout of the street and the positioning of the vehicles and personnel.

1. Who the President is...

2. Where the President is...

3. Who should have access to the President...



Perimeter

Monitoring

Micro-perimeter

Controls

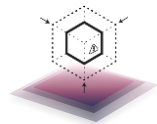
Protect surface

5-Steps to Deploying Zero Trust

ZEROTRUST

 **paloalto**
NETWORKS®

5 Steps to Deploying Zero Trust



1. Define your Protect Surface



Next-Generation Firewall



Cortex™ Data Lake



Cortex™ XDR



Transformation Services



2. Map the transaction flows



Next-Generation Firewall



Cortex™ Data Lake



Cortex™ XDR



Traps



Transformation Services



3. Build a Zero Trust architecture



Next-Generation Firewall



Cortex™ Data Lake



Cortex™ XDR



Traps



GlobalProtect



Prisma Access



Transformation Services



4. Create Zero Trust Policy



Panorama



WildFire



Threat Prevention



URL Filtering



Traps



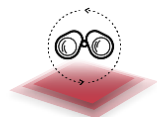
DNS Service



Prisma SaaS



Transformation Services



5. Monitor and maintain the network



Cortex™ Data Lake



Cortex™ XDR



AutoFocus



MineMeld



Demisto

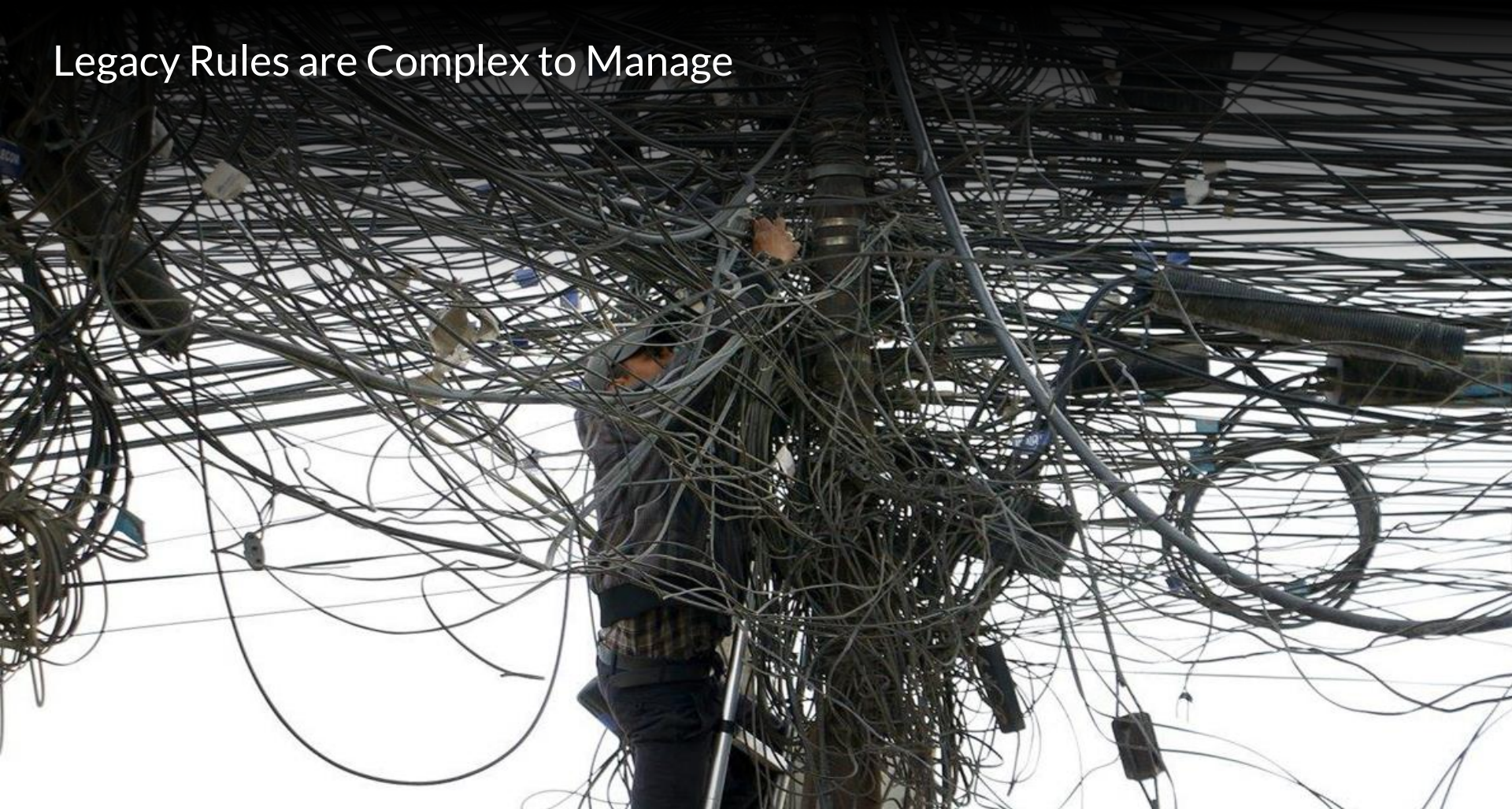


Prisma Cloud



Transformation Services

Legacy Rules are Complex to Manage



Create a Zero Trust Policy: The Kipling Method

Zero Trust policies must address *who, what, when, where, and how?*

Who	What	When	Where	Why	How	Action
User ID	App ID	Time	System Object	Classification	Content ID	
Sales	Salesforce	Working Hours	US	Toxic	SFDC_CID	Allow
Epic_Users	Epic	Any	Epic_Svr	Toxic	Epic_CID	Allow

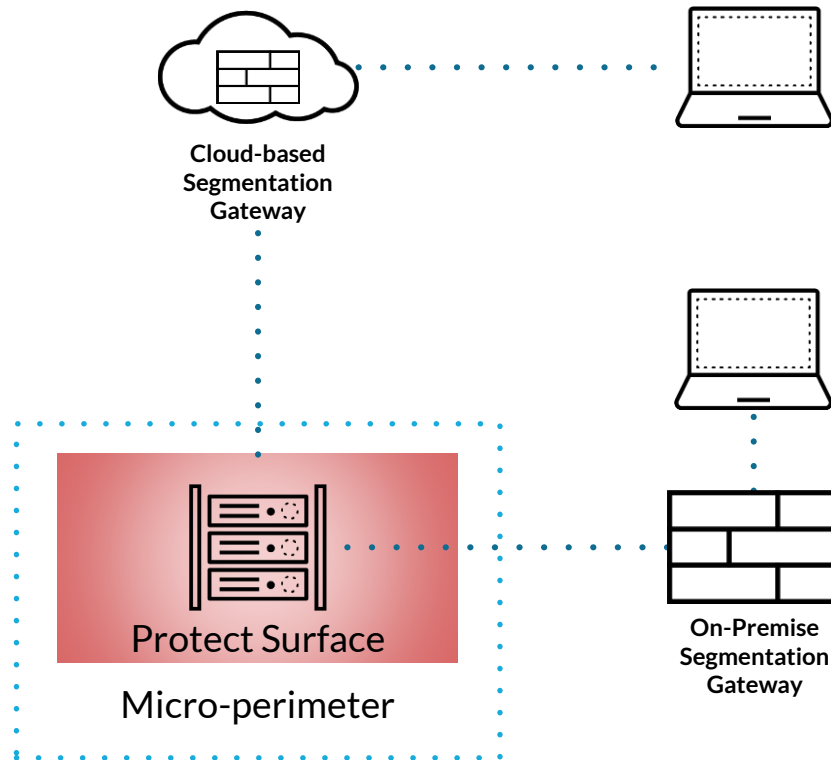
Use Cases

ZERO TRUST

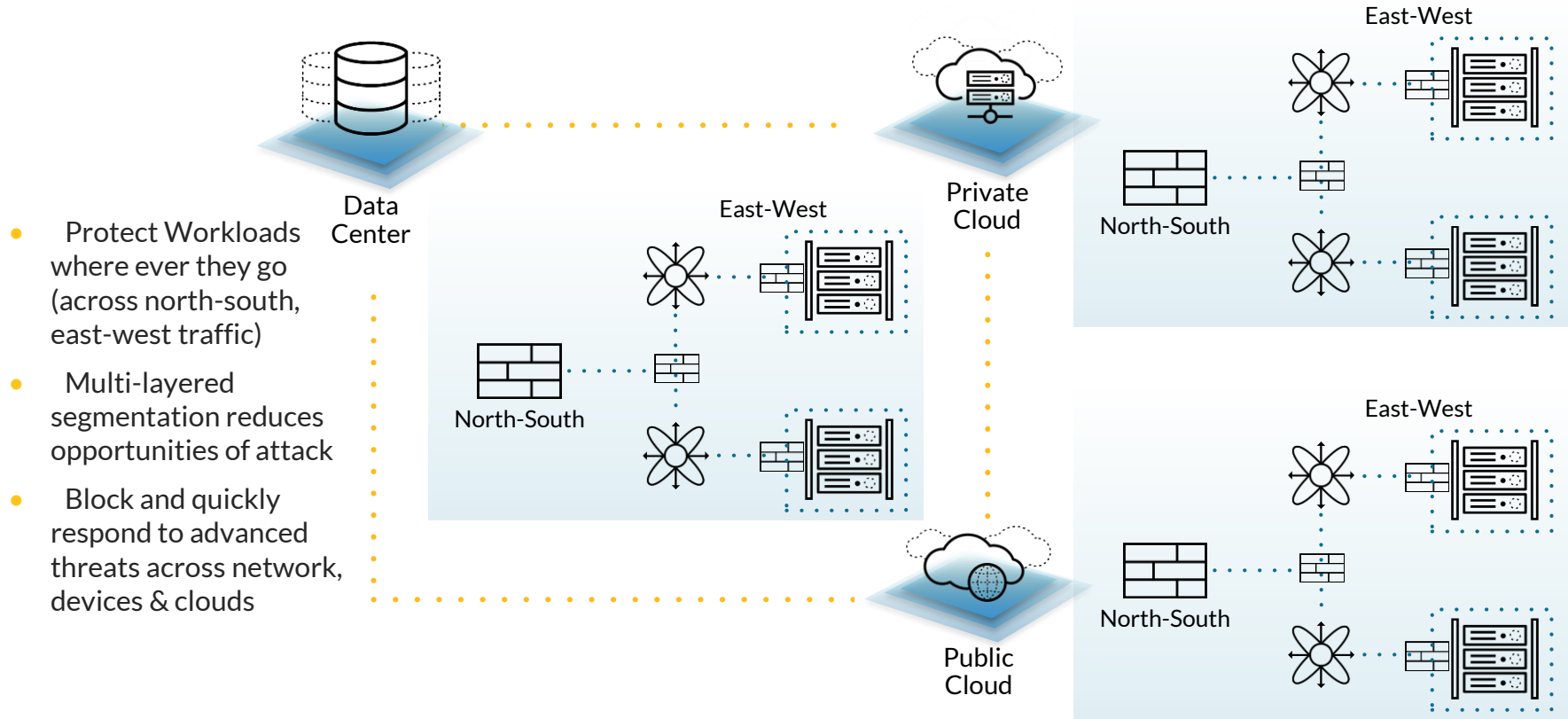
paloalto
NETWORKS®

Zero Trust for Mobile Workers

- Extending policy to devices attempting to access the protect surface
- Preventing employees or their devices from compromise by known and unknown threats

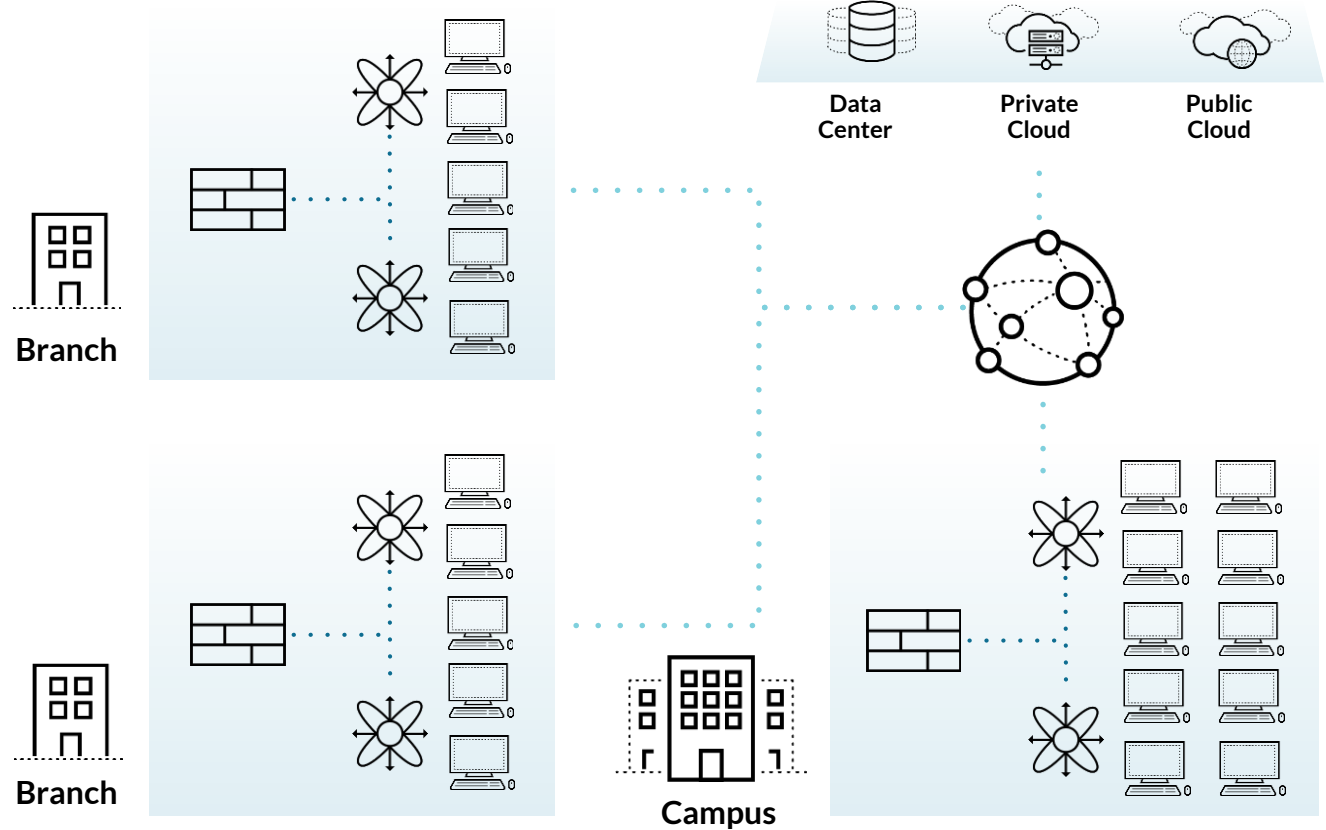


Zero Trust in A Multi-Cloud Environment



Zero Trust for Enterprise with Satellite Facilities

- Policy enforcement across users and devices accessing protect surface
- Prevent threats across branch, campus, datacenter and cloud



Customer Use Case

ZERO TRUST

paloalto
NETWORKS®

Customer Use Case

Overview:

- Due to the sensitive nature of their work the customer decided to look into a zero trust architecture for networking.

Customer Requirements:

- Complete visibility of **ALL** traffic from the inside out.
- Strict policy enforcement and continuous monitoring for attacks and abuse in isolated environments.

Customer Strategy:

- Control and monitor east west traffic within the data centers and between network locations.
- Control east west traffic between workstations on the same LAN segment (micro-segmentation).

Customer Architecture:

- 140 segmentation gateways across two networks with multiple instances of Panorama and Demisto (automation platform).
- Ability to deploy automated policies at scale and speed in an automated fashion.

Thank You

paloaltonetworks.com

npincever@paloaltonetworks.com

gcarlisle@paloaltonetworks.com

Twitter: @PaloAltoNtwks

ZEROTRUST

 **paloalto**
NETWORKS®